Patent
Docket No. 10971806-3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

APPEAL NO. _____

In re Application of:
Josh Hogan

Serial No. 09/783,112
Filed: February 14, 2001

Confirmation No. 2220
Group Art Unit: 2135
Examiner Thomas A. Gyorfi

For: METHOD AND APPARATUS FOR PERFORMING DATA ENCRYPTION AND ERROR CODE CORRECTION

APPEAL BRIEF

Hugh P. Gortler, Esq.

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

(949) 454-0898

INDEX

1. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company.

2. RELATED APPEALS AND INTERFERENCES

No appeals or interferences are known to have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

Claims 26-28 are pending in this application.

Claims 26-28 are rejected.

The rejections of claims 26-28 are being appealed.

4. STATUS OF AMENDMENTS

A final office action dated March 6, 2006 indicated that claims 26-28 were allowed, but claims 1 and 10 were rejected. In response to the final action, claims 1 and 10 were cancelled. A non-final office action was issued on August 3, 2006, and it withdrew the allowability of claims 27-28. An amendment was filed on Nov. 29, 2006 to address one of the issues raised in the August 3rd action (claim 27 was amended). The Nov. 29th amendment was entered. A notice of appeal and appeal brief were filed subsequent to the Nov. 29th amendment. The latest office action, dated 18 May 2007, attempts to re-open prosecution. No amendment was filed subsequent to the latest office action.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention addresses the problem of sending ECC-encoded blocks to a computer bus that is not secure. In a DVD drive, for instance, it might be desirable to send certain ECC-encoded blocks from the drive to a host computer for ECC-decoding. The host computer could perform more flexible error correction methods than the drive. For example, the DVD drive executes a default routine that is fast and that corrects a large majority of errors. Errors not corrected by the default routine are corrected by the host computer, using a more complex routine, such as a "heroic data recovery" routine.

The ECC blocks would be sent to the host computer's processor via a computer bus. However, if the computer bus is not secure, the unencrypted data in the blocks would be vulnerable to theft and unauthorized copying.

The ECC blocks could be encrypted before being sent to the computer bus. However, the integrity of the code words would be destroyed by encryption, whereby the host computer wouldn't be able to perform error correction.

The inventor has found that a specific type of encryption – XOR encryption – does not destroy the integrity of the code words. The ECC blocks can be XOR-encrypted in the drive, and sent to a host computer for error code correction. Moreover, the XOR encryption allows the host to perform the error code correction on the encrypted ECC blocks, without having to decrypt the ECC blocks. Error-corrected data, still encrypted, could then be sent downstream to an authorized device (e.g., an authorized DVD decoder card) for decryption.

Claim 26 recites a system comprising a computer bus, a host processor, and a drive. The host processor is programmed to perform error code correction. The drive provides an encryption mask, and performs a bitwise XOR of an

encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block. The drive provides the encrypted block to the computer bus, whereby an encrypted block can be sent to the host processor via the computer bus for error code correction.

Claim 27 recites a drive comprising a reader, and a controller for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data provided by the reader. A product of the bitwise XOR is an encrypted block.

Claim 28 recites a data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block.

Figure 1 of the application provides an example of the system of claim 26, the drive of claim 27 and the data controller of claim 28. A DVD drive 16 includes a reader 18 and the data controller 20. According to page 5, lines 11+, the reader 18 is operable to read RS-PC blocks stored on a DVD disc. According to page 6, lines 8+, a bitwise XOR of an encryption mask and a block of ECC-encoded data is then performed.

An RS-PC block, which is a type of ECC block, is illustrated in Figure 4 and described at page 7, line 29 to page 8, line 11. An example of bitwise XOR encryption of a line 501 of an RS-PC block and a line 502 of an encryption mask is illustrated in Figure 5 and described at page 8, lines 12+. According to page 11, lines 1+, the RS-PC block may be fully or partially encrypted.

According to page 6, lines 13+, the XOR-encrypted ECC block can be placed on a computer bus 12, where it is sent to a computer processor 14 for ECC decoding. The XOR-encryption provides protection against theft and unauthorized copying, even if the bus 12 is not secure. The XOR encryption does not destroy

the integrity of the ECC code words. Further, the XOR encryption allows the processor 14 to perform the ECC-decoding on the encrypted ECC block without performing decryption. Advantageously, the ECC-decoding can be performed on the encrypted ECC block, and the decryption can be performed downstream by a trusted entity (page 5, lines 2-3, and page 7, lines 11-22).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

a. Base claim 28 is rejected under 35 USC §102(a) as being anticipated by Koford.

b. Base claims 26-27 are rejected under 35 USC §103(a) as being unpatentable over Hibi in view of Koford.

7. ARGUMENTS

I

REJECTION OF CLAIM 28 UNDER 35 USC §102 AS BEING ANTCIPATED BY KOFORD U.S. PATENT NO. 4,377,862

The processor of claim 28 offers a solution to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying.

Koford does not teach or suggest a solution to that problem. Koford discloses a terminal service unit (TSU) that provides error control for asynchronous communication (col. 1, lines 11-14 and col. 3, lines 38-40). Tier 1 information, which enters the TSU, includes a series of 10-bit characters, where each incoming character includes 7 bits of data, and parity, start and stop bits (col. 4, lines 23-27). Within the TSU, the tier 1 information is reformatted into tier 2 information. The tier 2 information includes a series of characters, where each outbound character includes a group of the 7-bit data blocks (Figure 2 and col. 4, lines 50-56) and control information (col. 6, lines 40-44). The control information includes an 8-bit checksum, which comprises error control information (Figure 2 and col. 5, lines 43-45). The tier 2 information is then reformatted into tier 3 information by breaking down the tier 2 information into 8-bit sections (col. 6, lines 45-46).

The TSU includes a block 72 for performing encryption of known characters to produce a series of enciphered characters (col. 8, lines 55-61). The enciphered characters are used by a firmware block operating in cipher feedback mode to produce ciphertext characters from plaintext characters (col. 8, lines 61-68).

During operation, tier 1 packets flow from a user device (e.g., a computer

terminal) to the TSU (col. 8, lines 8+). When a character in a tier 1 packet is available at the receive buffer, it is delivered to either to a transmit buffer 90, or first to encipher/decipher module 88 and then to the transmit buffer (col. 8, line64 to col. 9, line 2). After the tier 1 data is encrypted, it is transformed into tier 2 data (col. 10, lines 31-39) . Thus, checksums are added after encryption has been performed.

Tier 3 packets flow from a distant TSU to a receiving TSU (col. 11, lines 1+). When a tier 3 packet is received, the receiving TSU examines the checksum to determine validity of the packet (col. 11, lines 11-14). Afterward, the decryption is performed (col. 11, lines 47+).

At no time is the checksum encrypted. Only data in the data blocks is encrypted and decrypted.

Koford does not teach or suggest encryption of ECC blocks (which ECC blocks include not only data, but also ECC code words).

Koford doesn't teach, suggest or even remotely hint that XOR encryption can preserve the integrity of ECC code words.

Koford isn't even relevant to the problem of sending ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. The applicant advances the art by offering a solution to the problem.

For these reasons, claim 28 should be allowed over Koford.

II
REJECTION OF CLAIMS 26-27 UNDER 35 USC §103 AS BEING UNPATENTABLE OVER HIBI IN VIEW OF KOFORD

The system of claim 26 and the drive of claim 27 offer solutions to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. Hibi and Koford, alone and in combination, do not teach or suggest a solution to this problem.

The latest office action acknowledges that Hibi does not teach or suggest a bitwise XOR of an encryption mask and a block of ECC-encoded data.

Argument I is incorporated by reference. Koford does not teach or suggest a bitwise XOR of an encryption mask and a block of ECC-encoded data. Therefore, the combined teachings of Hibi and Koford do not produce a system having all of the limitations of claim 26 or a drive having all of the limitations of claim 27. Accordingly, claims 26 and 27 should be allowed over the combined teachings of Hibi and Koford.

For the reasons above, the rejections of claims 26-28 should be withdrawn. The Honorable Board of Patent Appeals and Interferences is respectfully requested to reverse these rejections.

Respectfully submitted,

/Hugh Gortler #33,890/
Hugh P. Gortler, Esq.
Registration No. 33, 890

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

(949) 454-0898

Date: August 16, 2007

8. CLAIMS APPENDIX

26. (Previously presented) A system comprising:

a computer bus;

a host processor programmed to perform error code correction; and

a drive for providing an encryption mask, the drive performing a bitwise XOR of an encryption mask and a block of ECC-encoded data, a product of the bitwise XOR being an encrypted block; the drive providing the encrypted block to the computer bus, whereby an encrypted block can be sent to the host processor via the computer bus for error code correction.

27. (Previously presented) A drive comprising:

a reader; and

a controller for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data provided by the reader, a product of the bitwise XOR being an encrypted block.

28. (Previously presented) A data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data, a product of the bitwise XOR being an encrypted block.

9. EVIDENCE APPENDIX

None

10. RELATED PROCEEDINGS APPENDIX

None